$$
\begin{array}{rclcrclcrcl}
\phi \wedge \top & \Rightarrow & \phi & \quad & \top \wedge \phi & \Rightarrow & \phi & \quad & \perp \wedge \phi & \Rightarrow & \perp \\
\phi \wedge \perp & \Rightarrow & \perp & & \phi \vee \perp & \Rightarrow & \phi & & \perp \vee \phi & \Rightarrow & \phi \\
\top \vee \phi & \Rightarrow & \top & & \phi \vee \top & \Rightarrow & \top & & \neg \top & \Rightarrow & \perp \\
\neg \perp & \Rightarrow & \top & & \perp \rightarrow \phi & \Rightarrow & \top & & \top \rightarrow \phi & \Rightarrow & \phi \\
\phi \rightarrow \perp & \Rightarrow & \neg \phi & & \phi \rightarrow \top & \Rightarrow & \top & & & &
\end{array}
$$

FIG. 2.16 –

2.8 Diagrammes de décision binaire

Il s'agit d'une structure de données compacte utilisée pour représenter l'arbre sémantique associé à une formule, et donc en particulier toutes les interprétations qui la satisfont.

Si ϕ est une formules du calcul propositionnel, $\phi\{P \mapsto \top\}$ et $\phi\{P \mapsto \perp\}$ sont les formules obtenues en remplaçant P par $\top$ dans ϕ (resp. P par $\perp$ dans ϕ) puis en simplifiant par les règles de la figure 2.16.

Un *Graphe de décision* est un quadruplet (V, l, d, E) où V est un ensemble fini de sommets, l est une application de V dans $\mathcal{P} \cup \{\top, \perp\}$, d est une application de V dans $\mathcal{F}_0(\mathcal{P})$ et $E \subseteq V \times V$ tel que

1. G est enraciné et connexe : $\exists r \in V, \forall v \in V, v \neq r \rightarrow \exists v_1 = r, \ldots, v_n = v \in V, (v_1, v_2), \ldots, (v_{n-1}, v_n) \in E$
2. G est acyclique (pas de cycle $(v_1, v_2), \ldots (v_n, v_1) \in E$)
3. Le degré sortant de chaque noeud est 2 ou 0 :

$$\forall v \in V, |\{v' \in V \mid (v, v') \in E\}| \in \{0, 2\}$$

Deux graphes de décision G_1, G_2 sont *isomorphes* (ce qui est noté $G_1 \sim G_2$) s'il existe une bijection f de V_1 dans V_2 telle que :

1. pour tous $v_1, v_1' \in V_1$, $(v_1, v_1') \in E_1$ ssi $(f(v_1), f(v_1')) \in E_2$
2. pour tout $v_1 \in V_1$, $l(v_1) = l(f(v_1))$.

Definition 2.8.1 *Un* diagramme de décision binaire *(BDD) associé à la formule ϕ sur l'ensemble $\{P_1, \ldots, P_n\}$ de variables propositionnelles est un graphe de décision tel que $d(r) = \phi$ et tel que :*

- *Si $v \in V$ est tel que $l(v) \in \{\perp, \top\}$, alors v n'a pas de successeur et $d(v)$ est valide (si $l(v) = \top$) ou insatisfaisable (si $l(v) = \perp$).*
- *Si $l(v) \in \mathcal{P}$, alors v a exactement deux successeurs et les sous-graphes enracinés dans ces deux successeurs ne sont pas isomorphes.*
- *Si un noeud N est tel que $l(N) = P_i$, ses successeurs sont des noeuds N_1, N_2 tels que $\phi_1 = d(N_1) \models\mid d(N)\{P_i \mapsto \top\}$ et $\phi_2 = d(N_2) \models\mid d(N)\{P_i \mapsto \perp\}$ et $Var(\phi_1 \vee \phi_2) \subseteq \{P_j \mid j > i\}$.*

Exemple 2.8.1 Soit ϕ la formule $(P_1 \wedge P_2) \vee \neg((P_1 \wedge P_2) \vee \neg P_3)$. Un BDD associé est donné dans la figure 2.17 (par convention les fils gauche correspondent toujours à l'interprétation 1 de la variable du noeud correspondant).

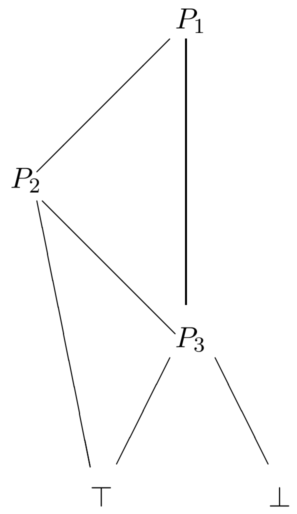

FIG. 2.17 – Un BDD associé à ϕ

L'intérêt des BDDs est d'une part une représentation compacte et, d'autre part, une représentation unique :

Theorem 2.8.1 (Canonicité) *Soient G, G' deux diagrammes de décision binaires (l'ordre sur les variables propositionnelles est fixé) associés respectivement aux formules ϕ et ϕ'. $G \sim G'$ si et seulement si $\phi \models\!\dashv \phi'$.*

<u>Preuve:</u>
Si $G \sim G'$, alors $\phi \models\!\dashv \phi'$ se montre par récurrence sur la taille de G : si G est réduit à une feuille, alors, ou bien c'est $\top$ et, par définition, ϕ et ϕ' sont valides. Ou bien c'est $\bot$ et, par définition ϕ, ϕ' sont insatisfaisables. Si maintenant G n'est pas réduit à une feuille, par hypothèse de récurrence, $\phi\{P \mapsto \top\} \models\!\dashv \phi'\{P \mapsto \top\}$ et $\phi\{P \mapsto \bot\} \models\!\dashv \phi'\{P \mapsto \bot\}$ d'où $\phi \models\!\dashv \phi'$.

Pour l'implication inverse, remarquons d'abord que, si ϕ est valide (resp. insatisfaisable), alors G est réduit à une feuille. En effet, si ϕ est valide, tout chemin conduisant à une feuille conduit à $\top$ (par récurrence sur le nombre de variables propositionnelles) et, comme aucun noeud n'a deux fils identiques, G ne peut contenir de sous-graphe dont les deux successeurs sont $\top$. Il en résulte que G est réduit à une feuille. (Le raisonnement est identique dans le cas où ϕ est insatisfaisable).

Si $\phi \models\!\dashv \phi'$. On montre $G \sim G'$ par récurrence sur le nombre de variables propositionnelles. S'il n'y en a pas, c'est immédiat. Sinon, si les deux graphes sont réduits à des feuilles, ils sont isomorphes. Si l'un d'eux au moins n'est pas réduit à une feuille, disons G, alors la racine est étiquetée par P_i et les deux fils de la racine correspondent aux formules $\phi\{P_i \mapsto \top\}$ et $\phi\{P_i \mapsto \bot\}$. Comme nous l'avons vu, dans ce cas, ϕ est satisfaisable et non valide. Il en est donc de même pour ϕ'. La racine de G' a donc deux fils correspondant aux formules $\phi'\{P_j \mapsto \top\}$ et $\phi'\{P_j \mapsto \bot\}$. On peut supposer sans perdre de généralité que

$j \geq i$. Si $j > i$, alors $P_i \notin Var(\phi')$ et donc $\phi\{P_i \mapsto \top\} \models\!\!\!\mid \phi\{P_i \mapsto \bot\}$ et, par hypothèse de récurrence, les deux fils de la racine de G sont alors isomorphes, ce qui est impossible. Donc $j = i$.

Comme $\phi \models\!\!\!\mid \phi'$ on a aussi $\phi\{P_i \mapsto \top\} \models\!\!\!\mid \phi'\{P_i \mapsto \top\}$ et $\phi\{P_i \mapsto \bot\} \models\!\!\!\mid \phi'\{P_i \mapsto \bot$ $\}$. Donc, par hypothèse de récurrence, les deux successeurs de la racine de G sont isomorphes aux deux successeurs de la racine de G' : $G \sim G'$. □

Exercice 56 (2)
Donner le BDD associé à la formule

$$(((A \to B) \wedge C) \to A) \vee \neg C$$

Avec l'ordre $A > B > C$, puis avec l'ordre $C > B > A$.

Exercice 57
L'objet de l'exercice est la construction de BDDs associés à des formules.

Tout d'abord, si on dispose de BDDs G_1, G_2 pour les formules $\phi\{P \mapsto \top\}$ et $\phi\{P \mapsto \bot\}$ il suffit de définir $G(\phi)$ par :

- Si $G_1 = G_2$ alors G_1
- Sinon $G(\phi)$ est le graphe de racine étiquetée par P et ayant deux fils respectivement G_1 et G_2.

On note alors $G = G_1 +_P G_2$.

Donner des algorithmes de construction de BDDs associés à $\phi_1 \wedge \phi_2, \phi_1 \vee \phi_2, \phi_1 \to \phi_2, \neg\phi_1$, supposant connus des BDDs associés à ϕ_1 et ϕ_2 respectivement.

$$\begin{array}{rclcrcl}
\phi \oplus \psi & \equiv & \psi \oplus \phi & \quad & \phi * \psi & \equiv & \psi * \phi \\
\phi \oplus (\psi \oplus \theta) & \equiv & (\phi \oplus \psi) \oplus \theta & & \phi * (\psi * \theta) & \equiv & (\phi * \psi) * \theta \\
\phi \oplus 0 & \equiv & \phi & & \psi * 1 & \equiv & \psi \\
\phi * (\psi \oplus \theta) & \equiv & (\phi * \psi) \oplus (\phi * \theta) & & & & \\
\phi \oplus \phi & \equiv & 0 & & \phi * \phi & \equiv & \phi
\end{array}$$

FIG. 2.18 – Equivalences structurelles

2.9 Anneaux Booléens

On considère dans cette partie une autre syntaxe du calcul propositionnel : on utilise les connecteurs $*$ (binaire), $\oplus$ (binaire), 1,0 (constantes). Les variables propositionnelles sont plutôt notées $X, Y, Z, \ldots$. L'ensemble des formules obtenues sur les variables propositionnelles $X_1, \ldots, X_n$ est alors noté $B(X_1, \ldots, X_n)$.

On interprète $*$ comme la conjonction, $\oplus$ comme le "ou exclusif" : $I \models \phi \oplus \psi$ si et seulement si $I \models \phi$ et $I \not\models \phi$ ou bien $I \not\models \phi$ et $I \models \phi$. 1 et 0 sont interprétés comme on s'y attend.

Les connecteurs habituels du calcul propositionnel s'expriment à l'aide de ceux-ci. Par exemple :

$$\phi \vee \psi \stackrel{\text{def}}{=} (\phi \oplus \psi) \oplus (\phi * \psi)$$

ou

$$\neg \phi \stackrel{\text{def}}{=} \phi \oplus 1$$

Les règles d'équivalence structurelle des formules sont données dans la figure 2.18. Ces règles engendrent une congruence notée $\equiv$. ($\equiv$ est la plus petite relation d'équivalence sur les formules contenant les équivalences de la figure 2.18 et telle que, si $\phi \equiv \psi$, alors $\phi \oplus \theta \equiv \psi \oplus \theta$ et $\phi * \theta \equiv \psi * \theta$ pour toute formule θ).

Lemme 2.9.1 *Si $\phi \equiv \psi$, alors $\phi \models\!\mid \psi$.*

<u>Preuve:</u>
Il suffit de le vérifier pour chacune des règles : comme $\equiv$ est la plus petite congruence les satisfaisant, $\equiv \subseteq \models\!\mid$. $\square$

L'avantage de cette notation pour le calcul propositionnel est d'avoir (au contraire de la forme clausale) une forme canonique : on oriente les équivalences de la figure 2.18 autres que l'associativité et la commutativité de la gauche vers la droite, obtenant ainsi un ensemble de règles de simplification $\Rightarrow$. On note encore $\Rightarrow^*$ la fermeture réflexive et transitive de $\Rightarrow$. (i.e. l'itération de la simplification).

Théorème 2.9.1 *Pour toute formule ϕ de $B(X_1, \ldots, X_n)$, il existe une unique (modulo l'associativité et la commutativité) formule $\phi \Downarrow$ telle que $\phi \Rightarrow^* \phi \Downarrow$ et $\phi \Downarrow$ est irréductible par ces règles.*

Les formules irréductibles sont ou bien 0, *ou bien des sommes de monômes distincts*

$$m_1 \oplus \ldots \oplus m_p$$

où chaque m_i *est ou bien 1 ou bien un produit* $X_{i_1} * \ldots * X_{i_k}$ *où* $X_{i_1}, \ldots, X_{i_k}$ *sont des variables propositionnelles distinctes.*

Preuve:
Les règles de simplification des formules qui se terminent : il suffit d'utiliser une interprétation simple dans les entiers, par exemple $g(\phi \oplus \psi) \stackrel{\text{def}}{=} g(\phi) + g(\psi) + 1$, $g(X_i) = 2 = g(1) = g(0)$, $g(\phi * \psi) = g(\phi) * g(\psi)$; g décroit stictement par application de n'importe quelle règle.

Les formes irréductibles sont bien des sommes de monômes : il suffit de vérifier qu'une règle s'applique à toutes les autres formules.

Montrons maintenant que la forme irréductible est unique : si une formule a deux formes irréductibles ϕ et ψ, alors $\phi \equiv \psi$ et donc, par le lemme 2.9.1, $\phi \models\!\!\!\!\dashv \psi$. On montre que $\phi = \psi$ par récurrence sur n (nombre de variables propositionnelles) :

- Si $n = 0$, alors $\phi = \psi = 1$ ou bien $\phi = \psi = 0$
- Si $n > 0$, on écrit les deux formules sous la forme $\phi = X_n * \phi_1 \oplus \phi_2$ et $\psi = X_n * \psi_1 \oplus \psi_2$ où $\phi_1, \phi_2, \psi_1, \psi_2$ ne contiennent pas X_n. $\phi \models\!\!\!\!\dashv \psi$ entraîne que $\phi\{X_n \mapsto 0\} \models\!\!\!\!\dashv \psi\{X_n \mapsto 0\}$ et $\phi\{X_n \mapsto 1\} \models\!\!\!\!\dashv \psi\{X_n \mapsto 1\}$, d'où $\phi_1 \models\!\!\!\!\dashv \psi_1$ et $\phi_2 \models\!\!\!\!\dashv \psi_2$ d'où, par hypothèse de récurrence, $\phi_1 = \psi_1$ et $\phi_2 = \psi_2$, et donc $\phi = \psi$.

$\square$

Corollaire 2.9.1 *Si* $\phi, \psi \in B(X_1, \ldots, X_n)$*, alors* $\phi \equiv \psi$ *si et seulement si* $\phi \models\!\!\!\!\dashv \psi$.

Corollaire 2.9.2 $B(X_1, \ldots, X_n)/\equiv$ *est un anneau commutatif isomorphe à* $\mathbb{Z}_2[X_1, \ldots, X_n]/\mathcal{I}$ *où* $\mathcal{I}$ *est l'idéal engendré par les polynômes* $(X_i^2 - X_i)$.

Chapitre 3

Calcul des prédicats

Nous abordons dans ce chapitre la *logique du premier ordre classique* aussi appelée *calcul des prédicats.*

Il y a plusieurs notations (calcul des séquents, systèmes à la Hilbert etc...)

3.1 Syntaxe

3.1.1 Les termes

$\mathcal{F}$ est un ensemble (fini) de symboles de fonction. Chaque symbole $f \in \mathcal{F}$ est muni d'une *arité* $a(f) \in \mathbb{N}$ qui fixe le nombre d'arguments.

$\mathcal{X}$ est un ensemble de symboles de variables (du premier ordre), disjoint de $\mathcal{F}$.

Un *arbre t étiqueté par $\mathcal{F}$* est consitué d'un *ensemble de positions $Pos(t)$* $\subseteq \mathbb{N}_+^*$ (mots sur les entiers non nuls) et d'une application de ce domaine dans $\mathcal{F}$ tels que :

- $Pos(t)$ est stable par préfixe : si $w \cdot i \in Pos(t)$, alors $w \in Pos(t)$. En particulier le mot vide $\epsilon \in Pos(t)$.
- Si $w \in Pos(t)$, $t(w) = f$, $a(f) = n$, alors $w \cdot i \in Pos(t)$ si et seulement si $i \in \{1, ..., n\}$.

On appelle *terme* (sur l'alphabet $\mathcal{F}$ et les variables $\mathcal{X}$) un arbre étiqueté par $\mathcal{F} \cup \mathcal{X}$, les symboles de $\mathcal{X}$ ayant une arité 0, et dont l'ensemble des positions est fini. L'ensemble des termes sur $\mathcal{F}$ et $\mathcal{X}$ est noté $T(\mathcal{F}, \mathcal{X})$.

Exemple 3.1.1 Si l'on suppose que $\mathcal{F}$ est composé des symboles $+, 0, s, eq, true, \&$ d'arités respectives $2, 0, 1, 2, 0, 2$, et $x \in \mathcal{X}$, quelques exemples d'éléments de $T(\mathcal{F}, \mathcal{X})$ sont donnés dans la figure 3.1. Les ensembles de positions de ces trois termes sont respectivement $\{\epsilon, 1, 1{\cdot}1, 2\}, \{\epsilon, 1, 2\}, \{\epsilon, 1, 1{\cdot}1, 1, {\cdot}2, 1{\cdot}2{\cdot}1, 1{\cdot}2{\cdot}2, 2\}$.

L'ensemble des variables d'un terme t, noté $\mathrm{Var}(t)$ est l'intersection de $\mathcal{X}$ et des étiquettes de t.

Exemple 3.1.2 Dans les exemples de la figure 3.1, le premier terme a pour ensemble de variables $\emptyset$ et les deux autres $\{x\}$.

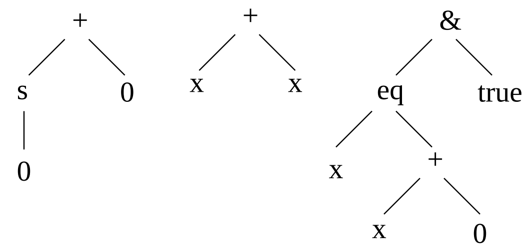

FIG. 3.1 – Exemples d'arbres finis

Les termes tels que $\mathrm{Var}(t)$ est vide sont appelés *termes clos*. L'ensemble des termes clos est noté $T(\mathcal{F})$.

On utilise habituellement une notation parenthésée pour les termes : si f est un symbole d'arité n, alors $f(t_1, \ldots, t_n)$ désigne le terme dont la racine est étiquetée par f et possède n fils, respectivement $t_1, \ldots, t_n$.

Exemple 3.1.3 Les termes de la figure 3.1 s'écrivent, en écriture parenthésée, $+(s(0), 0), +(x, x), \&(eq(x, +(x, 0)), true)$.

On utilise parfois l'écriture en notation infixée pour certains symboles usuels. Par exemple, $+(0, s(0))$ s'écrira aussi $0 + s(0)$.

Si $p \in D(t)$, le *sous-terme* de t à la position p, noté $t|_p$ est défini par récurrence sur la longueur de p : $t|_\epsilon = t$ et $f(t_1, \ldots, t_n)|_{i \cdot w} = t_i|_w$.

Exercice 58 (2)
Dans quel(s) cas est-ce que $T(\mathcal{F})$ est vide ? fini ?

3.1.2 Formules du premier ordre

$\mathcal{P}$ est de même un ensemble (fini) de symboles de prédicat, disjoint de $\mathcal{F}$ et de $\mathcal{X}$. Chaque symbole étant à nouveau muni d'une arité.

Les termes $P(t_1, \ldots, t_n)$ où $t_1, \ldots, t_n \in T(\mathcal{F}, \mathcal{X})$ et $P \in \mathcal{P}$ est d'arité n sont appelés *formules atomiques*.

Definition 3.1.1 *$CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$, ensemble des formules du premier ordre sur les symboles de prédicats $\mathcal{P}$, les symboles de fonction $\mathcal{F}$ et les variables $\mathcal{X}$ est le plus petit ensemble tel que :*
- $\bot, \top \in CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$
- *les formules atomiques sont dans* $CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$
- *Si* $\phi, \psi \in CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$ *et* $x \in \mathcal{X}$ *alors les formules suivantes sont dans* $CP_1(\mathcal{P}, \mathcal{F}, \mathcal{X})$ *:*

$$\phi \wedge \psi,\ \phi \vee \psi,\ \neg\phi,\ \phi \to \psi,\ \forall x.\phi,\ \exists x.\phi$$

Remarquons qu'on retrouve le calcul propositionnel lorsque tous les symboles de $\mathcal{P}$ sont d'arité 0.

Exemple 3.1.4 $\mathcal{F} = \{0(0), s(1)\}$, $\mathcal{P} = \{\geq (2)\}$. L'expression suivante est une formule du premier ordre :

$$\begin{array}{ll} & \forall x. \geq (x, 0) \\ \wedge & \forall x. \geq (s(x), x) \\ \wedge & \forall x, y. \geq (x, y) \rightarrow \geq (s(x), s(y)) \end{array}$$

Ici, comme dans la suite, nous abrégeons $\forall x.\forall y.\phi$ en $\forall x, y.\phi$.

Exemple 3.1.5 $\mathcal{F} = \{nil(0), cons(2)\}$, $\mathcal{P} = \{A(2)\}$. La formule suivante est censée définir la concaténation des listes :

$$\begin{array}{lll} \forall x, y, z, z_1.(& & A(nil, x, x) \\ & \wedge & A(y, z, z_1) \rightarrow A(cons(x, y), z, cons(x, z_1))) \end{array}$$

Exemple 3.1.6 La formule suivante n'est pas une formule du premier ordre :

$$\forall P.(P(0) \wedge \forall x.P(x) \rightarrow P(s(x))) \rightarrow \forall x.P(x)$$

On utilisera aussi certains symboles (de fonction ou de prédicat) en notation infixée. Par exemple, on se permettra d'écrire $a + b$ au lieu de $+(a, b)$ ou bien $a = b$ au lieu de $= (a, b)$.

Exemple 3.1.7 $\mathcal{F}$ est un ensemble fini de symboles de fonction avec leur arité. $\mathcal{P} = \mathcal{P}_0 \cup \{= (2)\}$ où $\mathcal{P}_0$ est un ensemble quelconque fini de symboles de prédicat avec leur arité. L'ensemble (fini) de formules suivants est appelé *axiomes de de l'égalité* :

$$\begin{array}{l} \forall x, y, z.x = y \wedge y = z \rightarrow x = z \\ \forall x, y.x = y \rightarrow y = x \\ \forall x.x = x \\ \forall x_1, \ldots, x_n, y_1, \ldots, y_n. \bigwedge_{i=1}^{n} x_i = y_i \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \\ \qquad\qquad\qquad\qquad \text{Pour tout } f \in \mathcal{F} \text{ d'arité } n \\ \forall x_1, \ldots, x_n. \bigwedge_{i=1}^{n} x_i = y_i \wedge P(x_1, \ldots, x_n) \rightarrow P(y_1, \ldots, y_n) \\ \qquad\qquad\qquad\qquad \text{Pour tout } P \in \mathcal{P}_0 \text{ d'arité } n \end{array}$$

Exemple 3.1.8 L'ensemble de formules suivant définit la théorie des ordres denses. On suppose les axiomes de l'égalité (donnée dans l'exemple précédent) et les deux symboles de prédicat binaires $=, \geq$ utilisés en notation infixée. On écrit en outre $a \neq b$ pour $\neg(a = b)$.

$$\begin{array}{l} \forall x, y, z.x \geq y \wedge y \geq z \rightarrow x \geq z \\ \forall x, y.x \geq y \wedge y \geq x \rightarrow x = y \\ \forall x.x \geq x \\ \forall x, y.(x \neq y \wedge x \geq y) \rightarrow (\exists z.x \geq z \wedge x \neq z \wedge z \geq y \wedge z \neq y) \end{array}$$